What is claimed is:

1. An apparatus for preventing illegitimate distribution of digital contents on Internet by employing a fingerprinting technique, comprising:

a first wavelet image obtained by performing a wavelet transformation (WT) to an original image of the digital contents, wherein the first wavelet image has a user information embedding region;

a second wavelet image obtained by performing a WT to the user information embedding region of the first wavelet image, wherein the second wavelet image composed of a discrete cosine (DC) region and high-frequency regions;

a high-frequency components removed image composed of the DC region and regions obtained by removing high-frequency components in the high-frequency regions of the second wavelet image, i.e., by setting high-frequency components other than the DC as "0", and subjected to an inverse WT (IWT) to be outputted as an IWT image; and

a user information embedding unit for embedding user information, which is provided from an operator, to the IWT image, thereby obtaining a user information embedded image with a new user information embedding region, comparing the user information embedding region of the first wavelet image with the new user information embedding region of the user information embedded image, and embedding the user

information to positions where a difference value between the user information embedding region and the new user information embedding region is small while minimizing a size change of the user information embedding region, to thereby reset the user information embedding region as the user information.

2. The apparatus of claim 1, wherein the new user information embedding region is determined by a length and an embedding intensity of a data sequence of the user information in order to minimize deterioration of image quality.

3. The apparatus of claim 1, wherein the user information embedding unit arranges difference values between the user information embedding region and the new user information embedding region according to the order of size and embeds the user information to positions of the arranged values in a magnitude order, staring from where a difference value between the user information and the user information is smallest.

4. A method for preventing illegitimate distribution of digital contents on Internet comprising the steps of:

performing a WT to an original image to obtain a first wavelet image;

determining a user information-embedding region in the first wavelet image and performing a WT to the user information-embedding region, thereby obtaining a second wavelet image;

removing high-frequency components from the second wavelet image by setting regions other than the user information-embedding region of a discrete cosine (DC) as "0", thereby obtaining a high frequency components removed image and performing an inverse WT (IWT) to the high-frequency components removed image, thereby obtaining an IWT image;

embedding user information provided from an operator to the IWT image to obtain a user information embedded image, comparing a user information embedding region of the user information embedded image with the user information embedding region and resetting the user information embedding region as a new user information embedding region LL_1, which is determined by a length and an embedding intensity of a data sequence of the user information in order to minimize deterioration of image quality; and

embedding the user information to a position where a difference value between the user information embedding region and the new user information-embedding region is small.

5. The method of claim 4, wherein an order number of the WT should be carefully selected since the user information is embedded to the DC region and the order number of the WT determines the size of the DC region.

6. The method of claim 4, wherein the DC region includes a largest amount of the user information if the DC region has a size equal to that of the original image and wherein if an n-order of WT is performed for an image having a size of M X N, a user information embedding region, LLn, to which the user information is to be embedded is determined from an equation as follows:

$$size(LL_n) = \frac{M}{2^n} \times \frac{N}{2^n} \quad .$$

7. The method of claim 6, wherein the size of the DC region is determined by considering a length and an embedding intensity of the data sequence of the user information and a degree of image deterioration due to the embedding of the user information data sequence.

8. The method of claim 4, wherein the new user information embedding region is obtained by low pass filtering the user information embedding region.

9. The method of claim 4, wherein positions of the new user information embedding region are determined by comparing a component of the user information embedding region and that of the new user information embedding region referring to the component of user information embedding region.

10. The method of claim 9, wherein if a component of the user information embedding region is larger than that of the new user information embedding region, the user information embedding region is considered as +1 while if a component of the user information embedding region is smaller than that of the new user information embedding region, the user information embedding region is regarded as -1.

11. The method of claim 10, wherein the size of the user information embedding region should be properly adjusted to satisfy the binary information because the new user information embedding region is obtained from the user information embedding region.

12. The method of claim 10, wherein an enough distance K should be secured between a user information embedding region and a new user information embedding region because the value of the user information embedding region can be changed by an arbitrary attack, wherein the new user

information embedding region is a DC region.

13. The method of claim 12, wherein the distance K is a variable that serves to determine the embedding intensity of the user information and wherein the distance K should be set to have a proper value by considering the fact that the image quality may be deteriorated if the distance value K is too big or too small.

14. The method of claim 12, wherein difference values between the user information embedding region and the new user information embedding region are arranged according to the order of size and data of the user information are sequentially embedded to positions of the arranged values in a magnitude order, starting from the smallest value; and wherein deterioration of image quality is greatly reduced by repeatedly performing a series of user information embedding processes as described above.

15. An apparatus for preventing illegitimate distribution of digital contents on Internet by employing a fingerprinting technique, comprising:

a first wavelet image obtained by performing a wavelet transformation (WT) to an original image of the digital contents, wherein the first wavelet image has a user information embedding region;

a second wavelet image obtained by performing a WT to the user information embedding region of the first wavelet image, wherein the second wavelet image composed of a discrete cosine (DC) region and high-frequency regions;

a high-frequency components removed image composed of the DC region and regions obtained by removing high-frequency components in the high-frequency regions of the second wavelet image, i.e., by setting high-frequency components other than the DC as "0", and subjected to an inverse WT (IWT) to be outputted as an IWT image; and

a user information embedding unit for embedding user information, which is provided from an operator, to the IWT image, thereby obtaining a user information embedded image with a new user information embedding region, and embedding the user information to a position determined by a random sequence generated from a location key in a blind information embedding system which does not use the first wavelet image, to thereby reset the user information embedding region as the new user information embedding region.

16. The apparatus of claim 15, wherein the random sequence [locat(K) ∈ {0,1}, $1 \le k \le S(LL_n)$] is set to have a probability defined in the following equation and wherein the user information is embedded to a position corresponding to "1" of the random sequence, LLn being a user information

embedding region:

$$P(1) = ui\_len / S(LL_n)$$
$$P(0) = 1 - ui\_len / S(LL_n)$$

17. The apparatus of claim 16, wherein ui_len and $S(LL_n)$ respectively represent the size of LL_n and the user information.

18. A method for preventing illegitimate distribution of digital contents on Internet comprising the steps of:

performing a WT to an original image to obtain a first wavelet image;

determining a user information-embedding region in the first wavelet image and performing a WT to the user information-embedding region, thereby obtaining a second wavelet image;

removing high-frequency components from the second wavelet image by setting regions other than the user information-embedding region of a discrete cosine (DC) as "0", thereby obtaining a high frequency components removed image and performing an inverse WT (IWT) to the high-frequency components removed image, thereby obtaining an IWT image;

embedding user information and a location key provided from an operator to the IWT image to obtain a user

information embedded image, thereby obtaining a user information embedded image with a new user information embedding region; and

embedding the user information to a position determined by a random sequence generated from a location key in a blind information embedding system which does not use the first wavelet image, to thereby reset the user information embedding region as the user information.

19. The method of claim 18, wherein the random sequence [locat(K) ∈ {0,1}, $1 \le k \le S(LL_n)$] is set to have a probability defined in the following equation and wherein the user information is embedded to a position corresponding to "1" of the random sequence, LLn being a user information embedding region:

$$P(1) = ui\_len / S(LL_n)$$
$$P(0) = 1 - ui\_len / S(LL_n)$$

20. The method of claim 18, wherein ui_len and $S(LL_n)$ respectively represent the size of LL_n and the user information.

21. The method of claim 16, wherein ui_len and $S(LL_n)$ respectively represent the size of LL_n and the user information.